Phishing Awareness Training

Phishing remains one of the most common and effective methods for data breaches and security incidents. This training will equip you with the knowledge and skills to identify, avoid, and report phishing attempts that target both you and your organization.

By the end of this training, you will be able to identify common types of phishing attacks, recognize red flags, understand the psychology behind these attempts, apply practical protection techniques, and follow proper reporting procedures when you encounter suspicious communications.

by Emmanuel Ateji

Types of Phishing Attacks

Email Phishing

Fraudulent emails appearing to come from legitimate sources like banks, colleagues, or service providers.

Spear Phishing

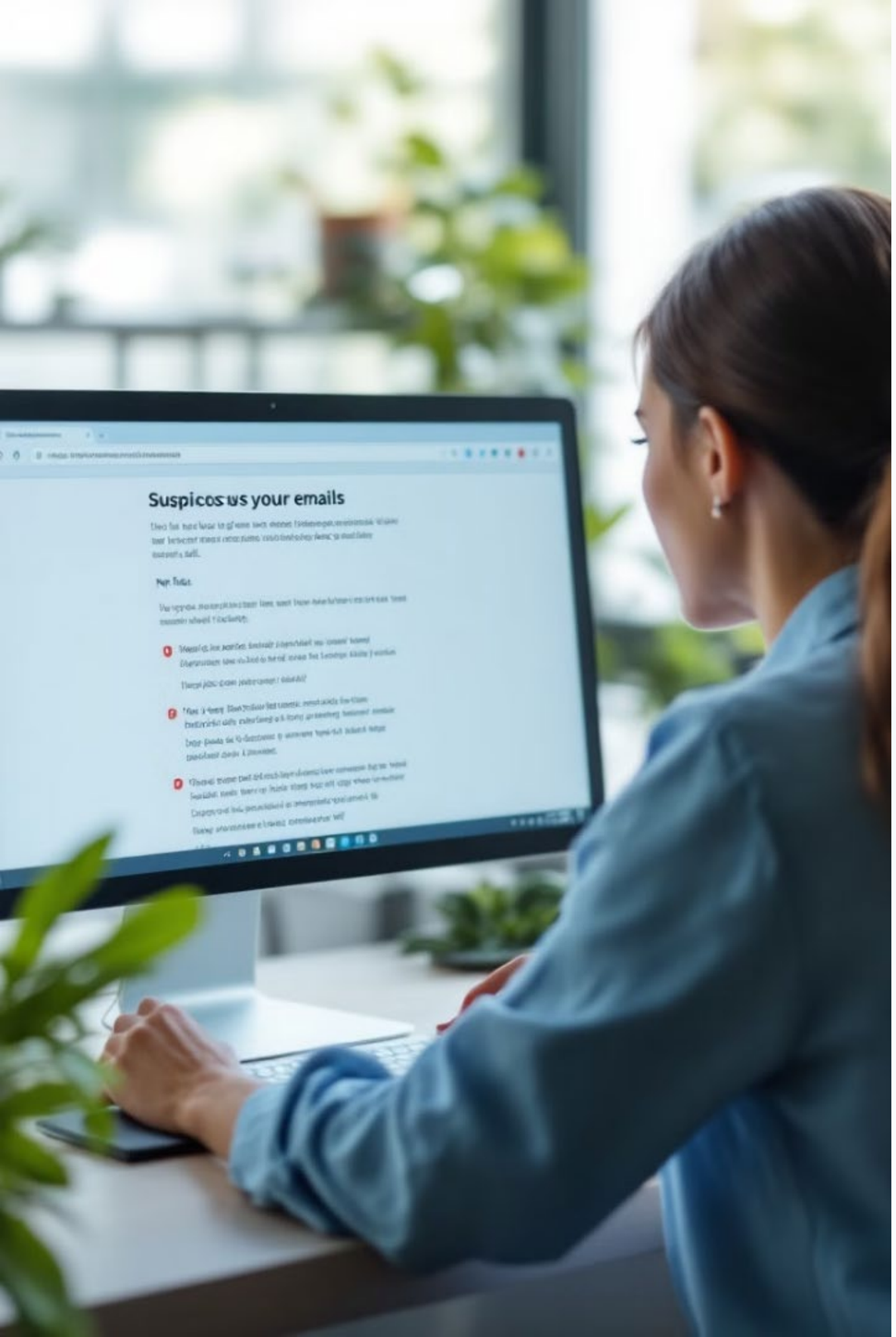
Targeted attacks directed at specific individuals using personalized information to appear more convincing.

Whaling

A form of spear phishing targeting high-profile executives or other high-value targets within an organization.

Vishing & Smishing

Using phone calls (vishing) or text messages (smishing) to trick victims into revealing sensitive information.



Red Flags: Spotting Phishing Attempts

Urgent or Threatening Language

Messages creating pressure to act quickly without thinking, often threatening account closure or security breaches.

Suspicious Email Domains

Mismatched or slightly altered email addresses (support@amaz0n - security.com instead of amazon.com).

Requests for Sensitive Information

Legitimate organizations rarely ask for passwords or personal information via email.

Suspicious Links & Attachments

Unexpected attachments or links that direct to websites with subtle URL differences.

The Psychology Behind Phishing

Fear

Threats about account closure or security breaches that trigger immediate action.

Helpfulness

Exploiting people's natural tendency to assist others who appear to need help.

Greed

Offers of money, prizes, or exclusive deals that seem too good to be true.

Trust

Impersonating trusted individuals or organizations to exploit established relationships.

Curiosity

Enticing subject lines or content that make you want to learn more and click through.

Practical Protection Techniques

Verify the Sender

Check the actual email address, not just the display name. Confirm through official channels if suspicious.

Hover Before Clicking

Check link destinations by hovering your cursor over them to reveal the actual URL.

Enable Multi-Factor Authentication

Use MFA wherever available to add an extra layer of security beyond passwords.

Keep Software Updated

Set automatic updates when possible and use security software with current protection.

Response Protocol: If You Suspect Phishing

Don't Interact

Don't click links, download attachments, or reply to the message. This prevents potential infection or confirmation that your address is active.

Report the Attempt

Forward suspicious emails to your organization's designated reporting address. Include details about why you found it suspicious.

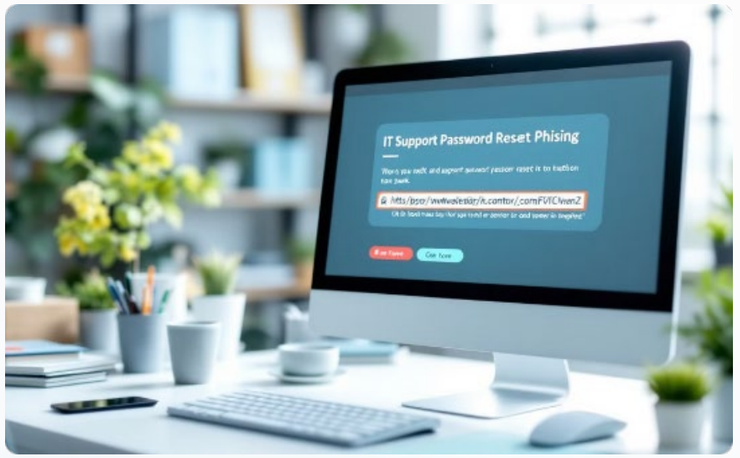
Take Action If Compromised

If you clicked a link or provided information, change affected passwords immediately, contact relevant financial institutions, and notify IT security.

Interactive Case Studies

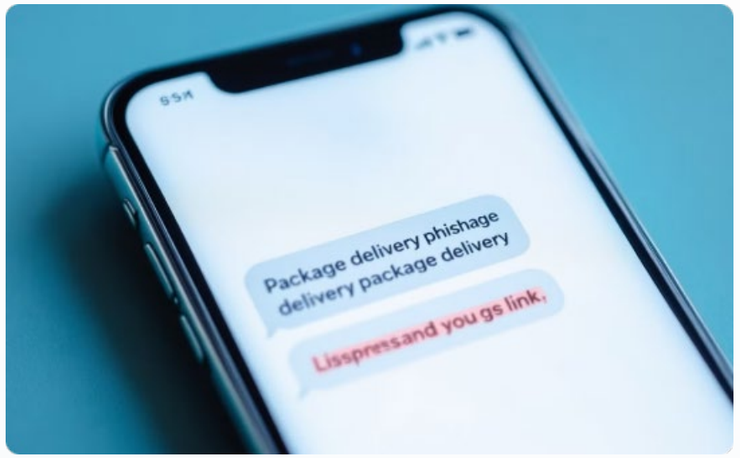
The Urgent Executive Request

Email seemingly from CEO requesting urgent wire transfer while traveling. Red flags: urgency, inability to verify, unusual request outside normal procedures. Correct response: Verify through established channels.



The IT Support Password Reset

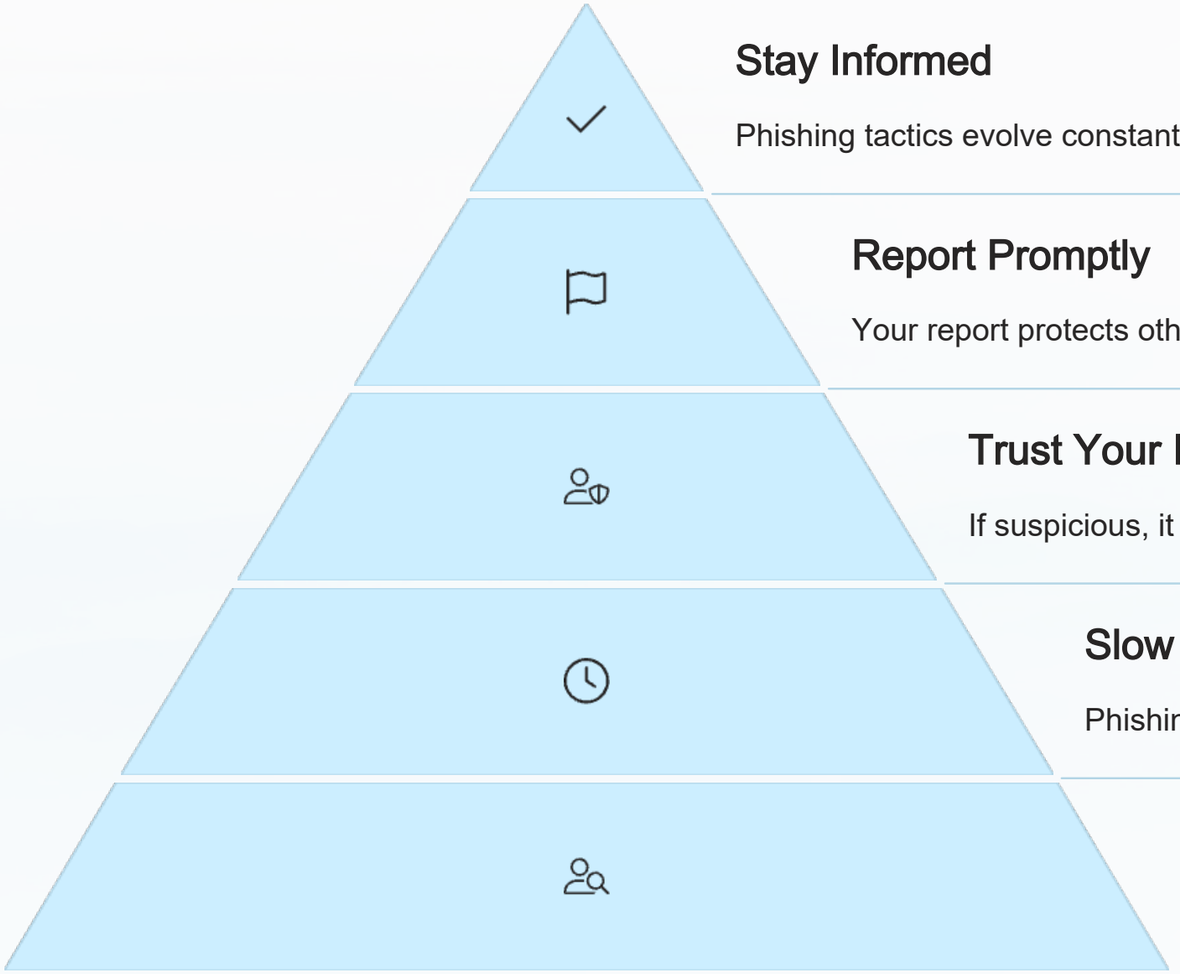
Email from "IT Support" about password expiration with reset link. Red flags: generic greeting, urgency, request for current password, suspicious URL. Correct response: Contact IT through official channels.



The Delivery Notification

SMS about package delivery issues with rescheduling link. Red flags: unexpected package, generic sender, short URL, requests for personal information. Correct response: Go directly to official website.

Key Takeaways & Resources



Stay Informed

Phishing tactics evolve constantly

Report Promptly

Your report protects others

Trust Your Instincts

If suspicious, it probably is

Slow Down

Phishing relies on quick responses

Verify Before Trusting

Confirm through official channels

Resources for further learning include CISA, FTC Consumer Information, and the Anti-Phishing Working Group (APWG). Contact your organization's IT Security team or visit the Internal Security Portal for organization-specific guidance and to report suspicious communications.